IN THE CLAIMS

The following amended claim set replaces all previous versions.

1. (Previously Amended) A method of excising a compromised node from a community of nodes capable of information sharing comprising:

for each group in a plurality of top tier groups in a top level tier, encrypting a new traffic encryption key using a top tier-group specific key encryption key, wherein the plurality of top tier groups excludes a group that includes the compromised node;

broadcasting the new traffic encryption key to each of the plurality of top tier groups in the top level tier; and

within the group that includes the compromised node, recursively broadcasting the new traffic encryption key to groups of nodes at a succession of lower tiers, until the compromised node is excised, wherein recursively broadcasting comprises:

for each of the groups of nodes in the succession of lower tiers, each of the groups of nodes excluding a lower tier group that includes the compromised node, encrypting the new traffic encryption key using a lower tier-group specific key encryption key.

3. (Original) The method of claim 1 wherein each tier in a progression of lower tiers comprises a plurality of groups, one group of the plurality of groups including the compromised node, and wherein recursively broadcasting comprises:

for each tier in the succession of lower tiers, broadcasting the new traffic encryption key to a subset of the plurality of groups, such that the compromised node does not receive the new traffic encryption key.

4. (Original) The method of claim 1 wherein recursively broadcasting comprises:

broadcasting the new traffic encryption key to a plurality of lower tier groups in a lower tier, the plurality of lower tier groups excluding a lower tier group that includes the compromised node; and

within the lower tier group that includes the compromised node, broadcasting the new traffic encryption key to a plurality of nodes in a lowest tier, wherein the plurality of nodes excludes the compromised node.

6. (Previously Amended) The method of claim 4 wherein the compromised node is a node coupled to a wireless communications system.

7. (Previously Amended) The method of claim 4 wherein the compromised node is a node coupled to the Internet.

8. (Previously Amended) A method of operating a key management center to excise a compromised node comprising:

from a list of top tier key encryption keys, selecting a top tier key encryption key that does not correspond to a group that includes the compromised node;

encrypting a new traffic encryption key using the top tier key encryption key, to produce a first encrypted traffic encryption key;

broadcasting a message that includes the first encrypted traffic encryption key;

from a list of lower tier key encryption keys, selecting a lower tier key encryption key that does not correspond to the group that includes the compromised node;

encrypting the new traffic encryption key using the lower tier key encryption key, to produce a second encrypted traffic encryption key; and

broadcasting a message that includes the second encrypted traffic encryption key.

9. (Original) The method of claim 8 further comprising repeating the actions in the method for all top tier groups except the group that includes the compromised node.

10. (Original) The method of claim 8 further comprising:

within the group that includes the compromised node, broadcasting the new traffic encryption key to a plurality of nodes excluding the compromised node.

11. (Original) The method of claim 10 further comprising:

within the group that includes the compromised node, broadcasting new tier group key encryption keys to the plurality of nodes excluding the compromised node.

12-15. (Canceled)